REMARKS

In the above-referenced Office Action, the Examiner rejected claims 11-22 under 35 U.S.C. § 103(a) as being unpatentable over Hall (U.S. Publication Number 2002/0138614 A1) in view of Slobodin et al. (U.S. Publication Number 2003/0072429 A1).

Independent claim 11 is directed to a method of communicating with a shared imaging apparatus connected to a computer network, wherein communication over said network is facilitated through use of network packets that requires, inter alia, instructing the networking hardware to accept information on the data channel from a user that owns the data channel. In the Office Action on page 2 Examiner alleged that Hall discloses instructing the networking hardware to accept information on the data channel from a user that owns the data channel (see abstract, fig. 5, [0031] to [0035]). Further, on page 8 the Examiner, while responding to the arguments made by the Applicants in response to the previous Office Action, states that Hall discloses instructing the networking hardware to accept information on the data channel from a user that owns the data channel (determination if the request for connection is secured and whether the network address is valid for further data processing, see abstract, fig. 5, [0031] to [0035]). The cited references, alone or in combination, fail to disclose or suggest this element of the claimed invention.

Hall in Fig. 1 discloses a network system 100 where the client systems 106, 108 are assigned network addresses by a network address provider 122 using the VPN Gateway 120. Fig. 2 shows the block diagram of the VPN Gateway 120 that has a processor 202 and a client proxy module that "performs the function of procuring a network address for a client and managing use of network address by the client." See page 3, paragraph 0027. Fig. 3 shows the programming logic performed by client proxy logic executed by processor 202 for connecting the clients 106 and 108 to a VPN network 104 that has the VPN Gateway and the network address provider. Initially, the client sends a request to the client proxy module for a secure connection that determines whether the request send by the client was in a protocol recognized by client proxy. If the request from the client was in the recognized protocol the client proxy would procure a network address for the client from the network address provider. If the network IP address provided by the network address provider is valid, the assigned network IP address is used to complete the secure virtual connection. In the Office Action, the Examiner has alleged that the "determination if the request for connection is secured and whether the network address is valid for further data processing" as disclosing "instructing the networking hardware to accept information on the data channel from a user that owns the data channel" in the claimed invention. However, in Hall the information (network address) is provided to the client (that accepts information, i.e., the IP address) on the data channel (124, 118, 116, 114 and 112 via VPN Gateway 120, See Fig. 3) from a network address provider that is a dynamic host configuration protocol server (DHCP) server and not a user, as in the claimed invention.

Further, in Hall the VPN gateway 200 as shown in Fig. 2 has an operator interface 206 that "may interface with a system operator by accepting commands and providing status information." See page 2, paragraph 0022. However, in Hall it is the client proxy module where the client proxy module "refers to software and/or hardware used to implement the functionality for procuring a network address for a client and managing the use" (page 3, paragraph 0029) present in the VPN gateway that is communicating with the client or the network address provider and Hall fails to disclose or suggests that the operator (user) is communicating (or sending information) either with the clients or with the network address provider and owning any of the the data channels. For at least these reasons, claim 11 is allowable

Additionally, independent claim 11 requires, inter alia, processing automatic Internet Protocol (IP) address negotiation network packets with the imaging apparatus firmware when the data channel is not owned, and processing second types of network packets, different from the automatic IP address negotiation network packets, by the networking hardware of said shared imaging apparatus when said data channel is owned. In the Office Action on page 2-3 the Examiner alleged that Hall discloses processing automatic Internet Protocol (IP) address negotiation network packets with the imaging apparatus firmware when the data channel is not owned, and processing second types of network packets, different from the automatic IP address negotiation network packets, by the networking hardware of said shared imaging apparatus when said data channel is owned (see [0035] to [0038]). Further, the Examiner alleged on page 9 that Hall discloses processing automatic Internet Protocol (IP) address negotiation network packets with the imaging apparatus firmware when the data channel is not owned (attempting to resend a predetermined number of times to get a valid IP address if the DHCP does return a valid network IP address, see [0035] to [0036]), and processing second types of network packets, different from the automatic IP address negotiation network packets, by the networking hardware of said shared imaging apparatus when said data channel is owned (if a valid network IP address is used to complete the secure connection, see [0035] to [0038]).

Hall further discloses that in case a valid IP address is not returned from the network address provider (DHCP server), then the client proxy module resends the request a predetermined number of times and, in case a valid IP address is not returned from the client, the client proxy sends a message to the client that the attempt to create a secure virtual connection to VPN network has failed. See page 4, paragraph 0035. In the Office Action, the Examiner alleged that the attempt by the client proxy module to obtain a valid IP address as disclosing processing automatic Internet Protocol (IP) address negotiation network packets with the imaging apparatus firmware when the data channel is not owned. Further, Hall discloses that if a valid IP address is received from the DHCP server the IP address is used to complete the secure virtual connection. In the Office Action, the Examiner alleged that the valid network IP address is used to complete the secure connection as disclosing processing second types of network packets, different from the automatic IP address negotiation network packets, by the networking hardware of said shared imaging apparatus when said data channel is owned. Applicants submit that the cited references, alone or in combination, fail to disclose or suggest these elements of the claimed invention.

First, Applicants assert that Hall only discloses a secure connection being obtained between the client and the network address provider and it fails to disclose or suggest owning of the data channel by the client, the network address provider or the VPN gateway.

Second, as discussed above, a number of attempts are being made by the client proxy module to obtain a valid IP address for the client and in case a valid IP address is obtained it is sent to the client to complete secure virtual connection between the client and the server. See Fig. 4. Assuming, arguendo, the request being sent for obtaining an IP address as a first type of network packet and the valid address being sent to the client for obtaining a secure connection as a second type of network packets, Applicants submit that during sending (processing) of both type of network packets, the virtual connection has identical state, i.e., in processing either the first data packet or the second data packet, the virtual network is disconnected and only after the second packet has been delivered is the virtual connection established. Rather, in the claimed invention the data channel is not owned (first state) when processing automatic internet protocol (IP) address negotiation network packet and is owned (second state) when the second type of network packet is processed.

Finally, independent claim 11 requires, inter alia, providing said shared imaging apparatus with networking hardware and providing said shared imaging apparatus with imaging apparatus firmware. In the Office Action on page 3, the Examiner admitted that Hall does not specifically disclose providing said shared imaging apparatus with networking hardware and providing said shared imaging apparatus with imaging apparatus firmware. However, the Examiner alleged that Slobodin et al. discloses providing said shared imaging apparatus with networking hardware, providing said shared imaging apparatus with imaging apparatus firmware (using two image source devices are used to generate image content concurrently and share the image content between the sites, see abstract, fig. 9, [0023] and [0075] to [0079]) and it would have been obvious to one of ordinary skill in the art at the time of the invention was made to implement Slobodin et al.'s teachings into the computer system of Hall to process data images because it would have established a data communication session via the data network for convenient transmission of image data between the sites. However, the cited references fail to disclose or suggest these elements of the claimed invention.

Fig. 9 of Slobodin et al. shows image sources 902 and 904 connected in a dataconferencing environment. Slobodin et al. discloses that the computer work stations 902 and 904 (referred as image source in Fig. 1) execute multi-source presentation management software using which image contents of these systems are displayed in a side-by-side manner on display screen. In alternate embodiments, Slobodin et al. discloses a display of image from a plurality of image sources. See page 8, paragraph 0076, 0077. The Examiner alleged the two image apparatus that can see the image content of the other system in a split screen as disclosing the shared imaging apparatus of the claimed invention. However, Slobodin et al. in paragraph 0060 specifically teaches that the cited reference eliminates the need for image data to be distributed to a centralized server and distributes and displays image "on-the-fly" nearly concurrently with their generation or playback at the image source: "Distribution and display of images on-the-fly also reduces image data storage required at each participating dataconferencing site. Dataconferencing systems in accordance with the present invention can also be configured so that no residual image data is left at participating sites after termination of the dataconferencing session." Applicants submit that as Slobodin et al. specifically teaches not to store image data (on the server or even after the data conference is over) the image sources are sending image data to each other using the data network and therefore these image sources cannot act as a "shared" imaging apparatus, as in the claimed invention.

Second, the Examiner alleged that the "processing automatic Internet Protocol (IP) address negotiation network packets with said imaging apparatus firmware" step of the claimed invention is being disclosed by "attempting to resend a predetermined number of times to get a valid IP address if the DHCP does not return a valid network IP address" of the cited reference. As discussed above the resending of request to obtain a valid network address in Hall is being performed by the client proxy module that is present in the program partition of the VPN gateway. See page 4, paragraph 0035. As admitted by the Examiner, Hall fails to disclose the imaging apparatus firmware and if the image source of Slobodin et al. is placed in the system of Hall, Applicants fail to understand that how the process of obtaining the IP address for a client and obtaining a connection between a client and a network address provider being performed by the VPN gateway would be performed by the image source of Slobodin et al.

Thus, claim 11 is allowable for at least these reasons.

Claims 12-22, which depend from allowable independent claim 11, are allowable for at least the same reasons. Further, these claims have additional limitations that make them allowable over the cited references.

For example, claim 17 requires, inter alia, that said second types of said network packets comprise imaging data. The Examiner alleged that Hall does not specifically disclose imaging data. However, Slobodin et al. discloses imaging data (using two image source devices are used to generate image content concurrently and share the image content between the sites, see abstract, fig. 9, [0023] and [0075] to [0079]) and it would have been obvious to one of ordinary skill in the art at the time of the invention was made to implement Slobodin et al.'s teachings into the computer system of Hall to process data images because it would have established a data communication session via the data network for convenient transmission of image data between the sites. The cited reference fails to disclose or suggest this element of the claimed invention. Applicants assert that the Examiner is not consistent in his allegation regarding "second type of network packets." The Examiner on page 9 alleged that "a valid network IP address received from the DHCP Server" in Hall as disclosing "second type of network packet" of the claimed invention, whereas with respect to claim 17 the Examiner alleged "image content present in the image source devices" of Slobodin et al. as disclosing the "second type of network packet." Thus, this claim is allowable for this additional reason.

Applicants assert that in light of the foregoing remarks this application is in condition for allowance and early passage of this case to issue is requested. The Examiner is invited to telephone the undersigned in the event the Examiner would like to discuss the merits of the application or this Response.

If there are any other fees not accounted for above, the assignee of present application, Lexmark International, Inc., hereby authorizes the Commissioner to charge any such fees, including any extension of time fees, to the account of Lexmark International, Inc., Deposit Account No. 12-1213.

Respectfully submitted,

Neill R. Kahle, Jr.
Registration No. 50,383
Lexmark International, Inc.
Intellectual Property Law Department
740 West New Circle Road
Bldg. 082-1
Lexington, KY 40550
Date: Sept. 19, 2008